Techniques and Issues in Multicast Security

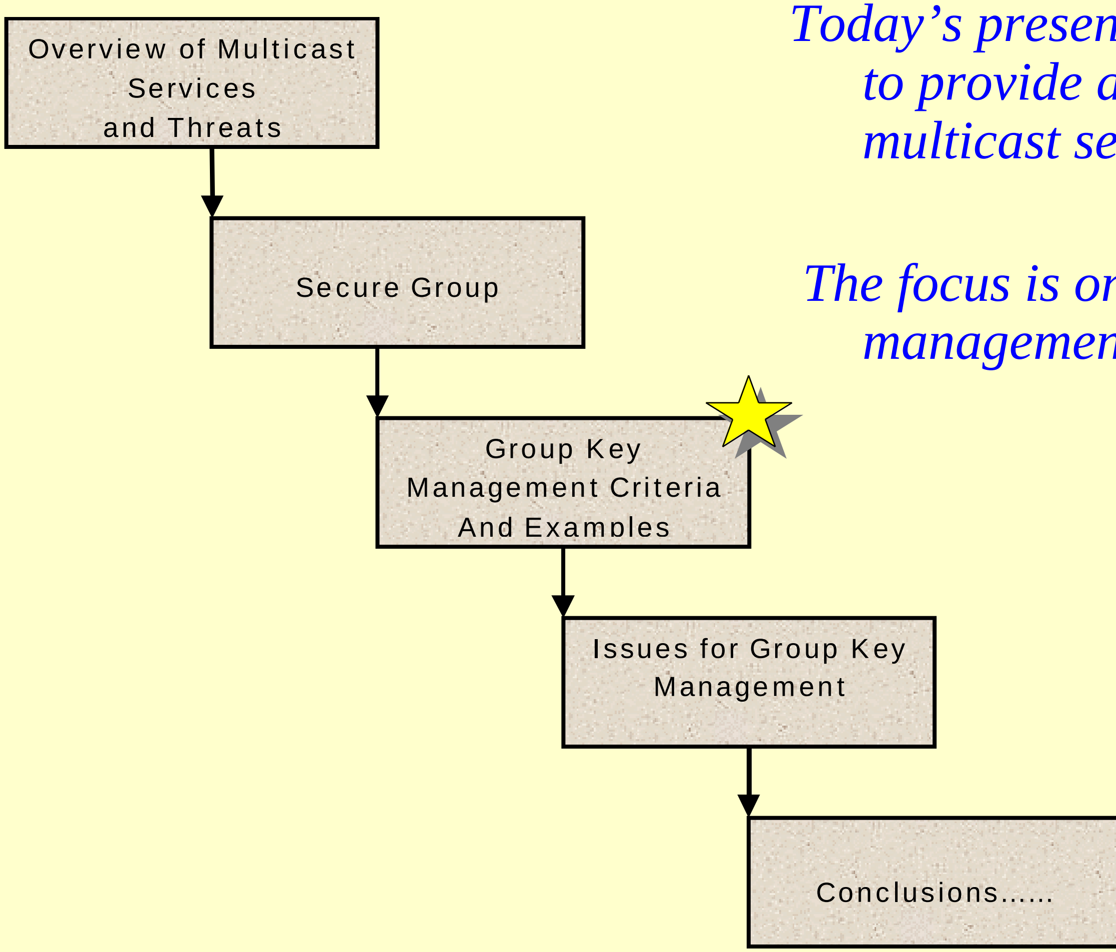
Presented for MILCOM 98

October 21, 1998

Peter S. Kruus
Naval Research Laboratory
kruus@itd.nrl.navy.mil

Joseph P. Macker
Naval Research Laboratory
macker@itd.nrl.navy.mil

Today's Presentation…..

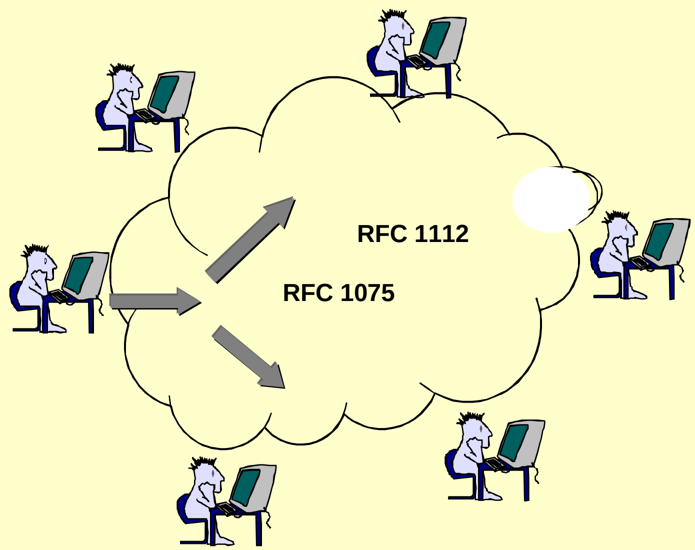


Today's presentation is intended to provide a overview of multicast security issues.

The focus is on group key management architectures.

Overview of IP Multicast Service

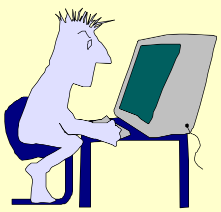
- IP multicast is an efficient means of distributing data to a *group* of participants.
- A sender need only transmit one copy of a datagram for the entire group.
- Multicast supports both *one-to-many* and *many-to-many* service.
- Multicast supports dynamic group communications:
  - Participants may join or leave a session at any time during its lifetime.
  - Knowledge of group's IP multicast address is required to join.



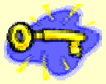
- Raw transport service is unreliable UDP/IP.
- Some RFC's which define IP multicast:
  - RFC-1112 (IP Multicast)
  - Multicast Routing: RFC-1075 (DVMRP), RFC-1584 (MOSPF), Other (e.g., CBT, PIM).

Threats to Multicast Traffic

- Multicast traffic is susceptible to the same threats as unicast traffic:
  - Eavesdropping, unauthorized creation and destruction of data, denial of service, illegitimate use of data.
- The typical security services (e.g., confidentiality, integrity, authentication) can be applied to traffic to counter these threats:
  - Security at the network layer using IPSEC mechanisms.
  - Security at the application layer for true end-to-end security.



- Because the scope of a multicast session can be large, these threats can be magnified:
  - Traffic can traverse multiple networks.
  - Large groups are more vulnerable to compromise.



Security concerns can be abstracted into a *group key management* problem.
  - The keys used to secure the group traffic must be protected.

Secure Multicast Group

- *Participant registration and authentication mechanisms determine the type of multicast group:*
  - *Public* session often do *not* require registration or authentication. Only need IP address to join.
  - *Private* sessions require some form of registration. All participants are authenticated.
- *Secure Multicast Group* ⇨ *Private session* with <u>encryption</u>:
  - The secure multicast group is defined by its:
    - IP multicast address
    - Group keying material
  - The registration process defines the group by limiting access to group keying material:
    - Limit membership to paying customers
    - Limit membership to properly cleared personnel
  - Rely on strong authentication mechanisms (e.g., digital signatures) to positively identify participants.

The Secure Multicast Process

The creation and maintenance of a secure multicast session follows the following framework:

- Identify the need for a secure group.
- Define parameters for the secure session that support the group's security policy (e.g., security services, key length, crypto-algorithm).
- Determine whether assistance is required to handle registration and other keying responsibilities.
- Announce the session through posted advertisement or invitation.
- Register participants and distribute keying material.
- Perform maintenance functions including *session rekey*:
  - Rekey to replace *outdated* key material
  - Rekey to replace *compromised* key material
  - Rekey to maintain *perfect-forwards and backwards secrecy* (i.e., rekey every join and exit)

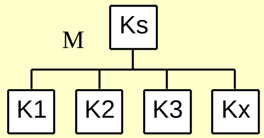
Group Key Management Criteria

Group keying schemes can be measured against the following criteria…..

- *Scalability* to support large groups (e.g., push cable application with +10,000 participants).
- *Robust* to survive link or component failures (e.g., a single key server).
- *Dynamic* rekeying to allow participants to enter and leave an active session while maintaining perfect-forwards/backwards secrecy.
- Prevention of *collusion* of disbanded participants from recreating any keying material.
- *Anonymity* in keying messages for privacy and to prevent traffic analysis.
- *Transmission efficiency* of keying messages.
- Storage *efficiency* of key material for participants and key server.
- *Computation efficiency* of key material for participants and key server.

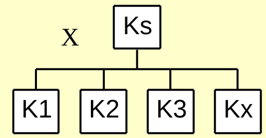
Group Key Management Architectures

Pairwise



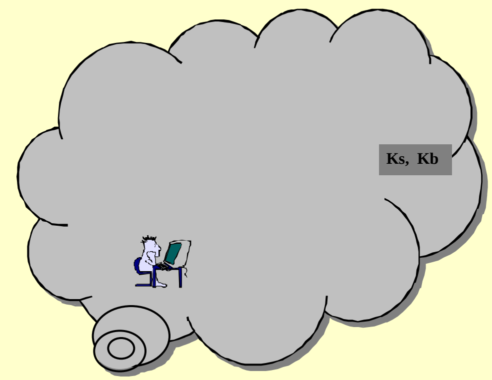
M = ({Ks}K1, {Ks}K2, {Ks}K3, ..., {Ks}Kx)

Broadcast

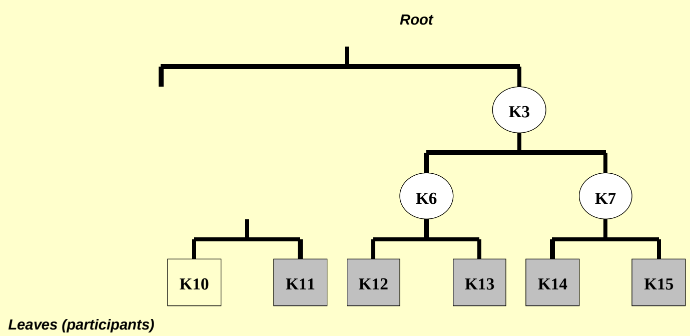


X = f ({Ks}K1, {Ks}K2, {Ks}K3, ..., {Ks}Kx)

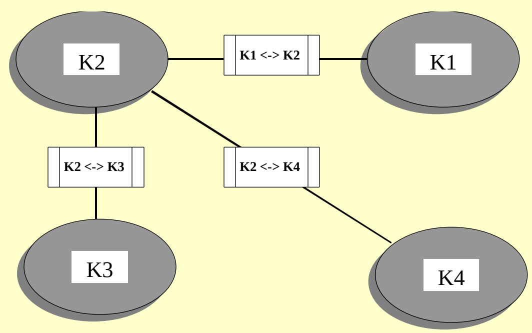
Distributed



Hierarchical



Subgroup



Other……

Comparison

Applying a strict criteria (large groups, perfect forwards/backwards secrecy):

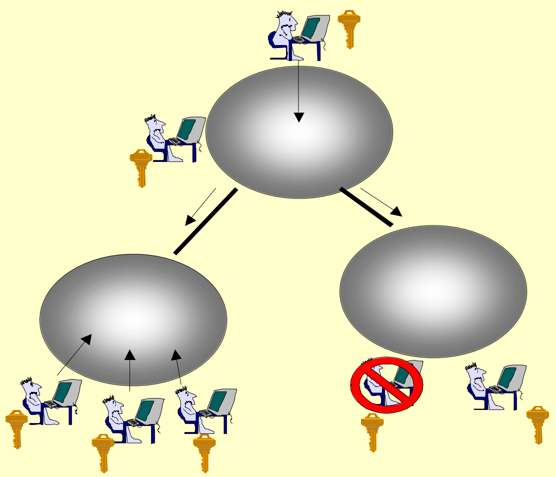
	Advantages	Disadvantages
Pairwise[1]	• Simple and straight forward approach.	• Not scalable to large groups. • Not efficient for providing perfect forwards/backwards secrecy.
Hierarchical[2]	• Scales logarithmically because of hierarchical design.	• Changes in group membership require group key to change. • Addressing required for key material.
Broadcast[3]	• Anonymity for rekey. • Common rekey package.	• Processing may approach pairwise techniques.
Distributed[4]	• Robust -> any active participant can distribute key material.	• Trust is distributed. • Membership lists or CRLs must be synchronized.
Subgroup[5]	• Membership changes only affect subgroup level.	• Architecture is not inherently robust.

Example group key architectures:

1. [GKMP]
2. [OWFT], [Wall], [Car]
3. [Lock]
4. [DiRK]
5. [Iolus]

Issues

- Multicast *security services* can suffer from scalability problems as the group size becomes large:
  - Maintaining perfect forwards/backwards secrecy becomes difficult as group *size* increases and membership *turnover rates* increases.

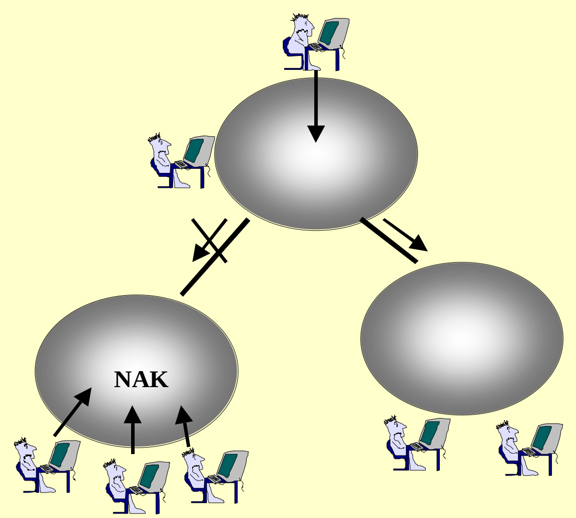


Dynamic membership creates perfect-secrecy problems.

- Centralized vs. Distributed key server:
  - *Centralized* → efficient for push applications, simpler key management, scalability problems
  - *Distributed* → robust, trust is distributed, key synchronization problems.

Issues *(continued)*

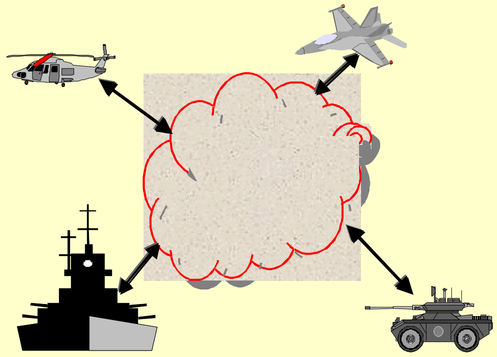
- Reliability is required for key distribution to ensure that all participants receive *rekey* material:
  - Raw IP multicast service is inherently *best effort.*
  - There are numerous reliable transport protocols that can be applied over of UDP.
  - Reliability can be either *source* or *receiver* oriented.
  - Reliable transport techniques have their own diverse performance characteristics that should be considered.
- Some reliable transport protocols can impose a hierarchy to handle requests for retransmission:
  - This hierarchy can introduce *third parties* that must be trusted by the group.



Message failures can create control message implosion problems.

Sample Keying Requirements for Tactical Military Networks

- Bandwidth constrained RF links require the *efficiency* found in multicast traffic:
  - Group key distribution should mimic multicast efficiency.
- Tactical networks must be *robust* to recover from mobile and dynamic link conditions:
  - Group key architecture should have distributed properties.
- Maintain perfect forwards and backwards secrecy:
  - Efficient rekey mechanisms.

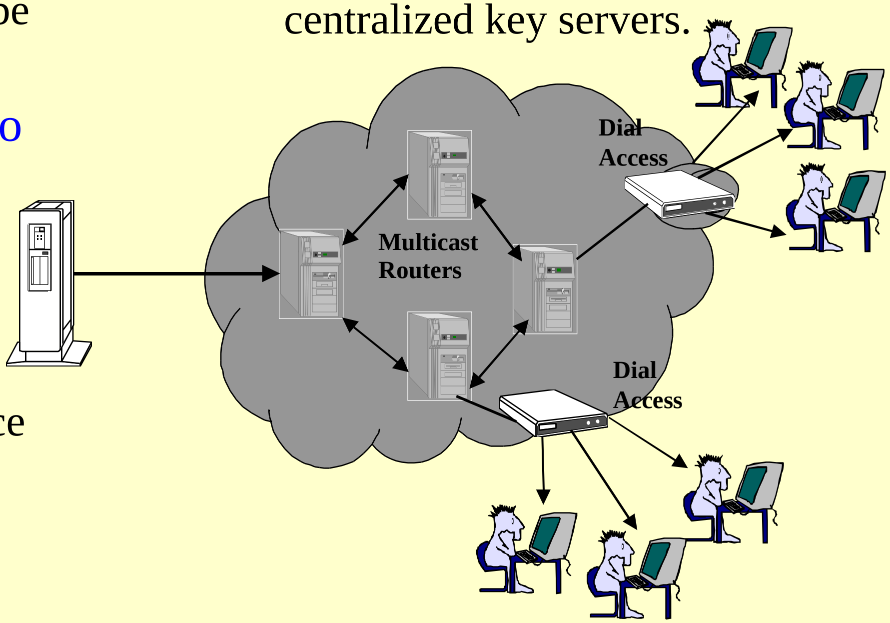


- Participant *anonymity* required to help prevent traffic analysis:
  - Group key architecture should employ *broadcast* qualities.
- *Reliability* mechanisms are required to ensure key material is received by all participants.
- Security Services:
  - Source Authentication
  - Confidentiality, integrity

Sample Keying Requirements for Commercial Networks

- Commercial applications have potential for large groups:
  - Require a scalable solution.
- Bandwidth constrained links for dial customers:
  - Group key distribution should be efficient.
- Participant *anonymity* required to for privacy:
  - Group key architecture should employ *broadcast* qualities.
- Security Services:
  - Confidentiality, integrity, source authentication

- *Reliability* mechanisms are required to ensure key material is received by all participants:
  - The absence of multicast return channels suggests centralized key servers.



Conclusions

- Outside forces play an important role in defining an efficient key management architecture:
  - Security policy can have a defining role.
  - Other protocol layers (e.g., reliable multicast) can influence design.
- Secure multicast requires tight access control:
  - Benefits from a well established PKI.
- Any group key management solution must also consider the user application it supports:
  - Commercial push services may benefit from centralized keying schemes.
  - Tactical distributed applications may require a more robust solution.
- Reasonable solutions balance the tradeoff's for both *communications* and *security* requirements for an intended network architecture.
- In summary, there is no "one-size fits all" solution.

References

[DiRK] *Distributed Registration and Key Distribution (DiRK)*, R. Oppliger and A. Albanese, Proceedings of the 12th International Conference on Information Security (IFIP SEC '96), Island of Samos (Greece), May 21-24, 1996, Chapman & Hall, London, pp. 199-208.

[WALL] *Key Management for Multicast: Issues and Architecture*, D. Wallner, E. Harder, and R. Agee, Internet-Draft, draft-wallner-key-arch-00.txt, 1 July 1997.

[GKMP] *Group Key Management Protocol (GKMP) Architecture*, H . Harney and C. Muckenhirn, RFC-2094, July 1997.

[Lock] *Secure Broadcasting Using the Secure Lock*, G .H. Chiou and W.T. Chen, IEEE Transactions on Software Engineering, v. SE-15, n. 8, August 1989, pp. 929-934.

[Car] *Efficient Security for Large and Dynamic Multicast Groups*, G. Caronni, M. Waldvogel, D. Sun, B. Plattner, Proceedings of the Seventh Workshop on Enabling Technologies (WET ICE '98), IEEE Computer Society Press, 1998.

[Iolus] *Iolus: A Framework for Scalable Secure Multicasting*, S. Mittra, Proceedings fo the ACM SIGCOMM '97, September 14-18 1997, Cannes, France.

[OWFT] *Key Establishment in Large Dynamic Groups Using One-Way Function Trees*, D. McGrew, A. Sherman, TIS Labs at Network Associates, TIS Report #0709, 2 June 1998.